**DOE CIO Guidance CS-4**

# U.S. Department of Energy

# Cyber Security Program

# VULNERABILITY MANAGEMENT GUIDANCE

**July 28, 2006**

1. PURPOSE.

   This Department of Energy (DOE) Chief Information Officer (CIO) Guidance provides guidance for the implementation of a Vulnerability Management process as described in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-40, *Creating a Patch and Vulnerability Management Program* and NIST SP 800-42, *Guideline on Network Security Testing*.

   The DOE CIO will review this guidance annually and update it as necessary. Senior DOE Management and their operating units may provide feedback at any time for incorporation into the next scheduled update.

2. SCOPE.

   This Guidance is provided additional information to Senior DOE Management for addressing the controls in DOE CIO Guidance CS-1, *Management, Operational, and Technical Controls Guidance* and DOE CIO Guidance CS-22, *National Security Systems Controls Guidance*, in their Program Cyber Security Plans (PCSPs). Specifically, this Guidance applies to the Risk Assessment controls in CS-1 and Intrusion Detection, Vulnerability Assessment, and Life Cycle Support controls in CS-22.

3. CANCELLATIONS.

   None.

4. APPLICABILITY.

   a. Primary DOE Organizations. This Guidance applies to all DOE Organizations listed in Attachment 1, *Primary Department of Energy Organizations to which DOE CIO Guidance CS-4 is Applicable*.

      Further, the DOE Under Secretaries, the NNSA Administrator, the Energy Information Administration, the Power Marketing Administrations, and DOE CIO (hereinafter referred to as Senior DOE Management) may specify and implement supplemental requirements to address specific risks, vulnerabilities, or threats within their subordinate organizations and contractors (hereinafter called operating units), and for ensuring that those requirements are incorporated into contracts.

   b. Exclusions. Consistent with the responsibilities identified in Executive Order (E.O.) 12344, the Director of the Naval Nuclear Propulsion Program will ensure consistency through the joint Navy and DOE organization of the Naval Nuclear Propulsion Program and will implement and oversee all requirements and practices pertaining to this DOE Guidance for activities under the NNSA Administrator's cognizance.

c. DOE Unclassified Systems. Senior DOE Management PCSPs are to address this Guidance for all systems hosting unclassified information. DOE M 471.3-1, *Manual for Identifying and Protecting Official Use Only Information,* and DOE M 471.1-1, *Identification and Protection of Unclassified Controlled Nuclear Information Manual,* provide additional information for identifying unclassified information requiring protection.

d. National Security Systems. Senior DOE Management PCSPs are to address this Guidance for all DOE National Security systems. Executive Order 12829 (E.O. 12829), which established the National Industrial Security Program; the requirements of the *National Industrial Security Program Operating Manual (NISPOM);* the Atomic Energy Act of 1954, which established Restricted Data information; DOE CIO Guidance CS-22, *National Security Systems Controls Guidance;* and NIST SP 800-59, *Guidelines for Identifying an Information System as a National Security System,* provide additional guidance for identifying National Security systems.

5. IMPLEMENTATION.

This guidance is effective 30 days after issuance. However, DOE recognizes that this guidance cannot be implemented into Senior DOE Management PCSPs overnight. Except as noted below, DOE expects that Senior DOE Management shall address the criteria in this document within 90 days of its effective date. If Senior DOE Management cannot address all of the criteria by the scheduled milestone, Senior DOE Management are to establish a Plan of Actions and Milestones (POA&Ms) for implementation of this Guidance into their PCSPs.

6. CRITERIA.

a. Program Cyber Security Plans. Senior DOE Management PCSPs are to be consistent with the criteria in DOE OCIO Guidance CS-1, *Management, Operational, and Technical Controls*. To ensure consistency with these controls, Senior DOE Management PCSPs are to direct operating units to develop, document, and implement vulnerability management policies and procedures consistent with the following criteria and commensurate with the level of security required for the organization's environment and specific needs.

(1) Vulnerability management activities including the processes for analyzing, detecting, communicating, and remediating vulnerabilities as well as the interfaces to incident management and configuration management processes

(2) The roles and responsibilities of all key personnel, including those identified in DOE CIO Guidance CS-2, *Certification and Accreditation Guidance,* are responsible for decisions and activities regarding vulnerability management.

(3) Awareness, training, and education requirements for all key personnel responsible for vulnerability management activities.

(4) A vulnerability management process addressing –

(a) An inventory of information technology resources, including hardware, operating systems, and software applications used in the organization

(b) Identification and dissemination of vulnerability information

(c) Remediation strategies and processes, including roles and responsibilities for remediating identified vulnerabilities within the organization

(d) Prioritization of vulnerability remediations

(e) Vulnerability scanning

i. The organizational element(s) responsible for vulnerability scanning.

ii. The identification and prioritization of scanning targets.

iii. Alternate examination methodologies for resources for which operations/production cannot be interrupted (e.g., SCADA systems)

iv. Risk-based standards establishing scan frequency, techniques, and technology(ies).

v. Identification of those resources that cannot be scanned from a central network location.

(f) A standardized vulnerability naming scheme

(g) The documentation of vulnerabilities, including corrective action plans, POA&M documentation, and Incident Management, as appropriate.

(5) A uniform patch management and flaw remediation process addressing –

(a) Roles and responsibilities of all key personnel, including those identified in DOE CIO Guidance CS-2, *Certification and Accreditation Guidance*, responsible for decisions and activities regarding patch management activities.

(b) Patch prioritization and testing.

(c) Automated/ manual patch deployment.

(d) Identification of those resources that cannot be patched from a central network location.

(e) Prioritization, coordination, and implementation of vulnerability remediation and/or mitigations.

(f) Maximum time(s) for patch testing and installation.

(g) Patch installation verification processes and methods.

(h) Integration with Configuration Management processes.

(6) Communication and coordination processes concerning –

(a) Internal and external reporting of vulnerabilities and remediations.

(b) Interface with processes in DOE CIO Guidance CS-6, *Plans of Action and Milestones Guidance*.

(c) A process for identifying, documenting, and communicating lessons-learned concerning vulnerability scanning and remediation.

7. REFERENCES.

References are listed in DOE CIO Guidance CS-1, *Management, Operational, and Technical Controls Guidance*.

8. DEFINITIONS.

Acronyms and terms applicable to all DOE CIO Guidance are included in DOE CIO Guidance CS-1, *Management, Operational, and Technical Controls Guidance*.

9. CONTACT.

Questions concerning this Guidance should be addressed to the Office of the Chief Information Officer, (202) 586-0166.

# ATTACHMENT 1

## PRIMARY DEPARTMENT OF ENERGY ORGANIZATIONS TO WHICH DOE CIO GUIDANCE CS-4 IS APPLICABLE

Office of the Secretary
Office of the Chief Financial Officer
Office of the Chief Information Officer
Office of Civilian Radioactive Waste Management
Office of Congressional and Intergovernmental Affairs
Departmental Representative to the Defense Nuclear Facilities Safety Board
Office of Economic Impact and Diversity
Office of Electricity Delivery and Energy Reliability
Office of Energy Efficiency and Renewable Energy
Energy Information Administration
Office of Environment, Safety and Health
Office of Environmental Management
Office of Fossil Energy
Office of General Counsel
Office of Hearings and Appeals
Office of Human Capital Management
Office of the Inspector General
Office of Intelligence and Counterintelligence
Office of Legacy Management
Office of Management
National Nuclear Security Administration
Office of Nuclear Energy
Office of Policy and International Affairs
Office of Public Affairs
Office of Science
Office of Security and Safety Performance Assurance
Bonneville Power Administration
Southeastern Power Administration
Southwestern Power Administration
Western Area Power Administration